

## UNITED STATES DISTRICT COURT

for the  
District of South Carolina

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*INFORMATION ASSOCIATED WITH EMAIL ACCT.  
wilkinswendell870@gmail.com MAINTAINED BY GMAIL  
STORED AT PREMISES CONTROLLED BY GOOGLE

Case No. 2:18-CR-905

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attached Affidavit

located in the \_\_\_\_\_ District of \_\_\_\_\_ South Carolina \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 873	Extortion
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 880	Receiving Proceeds of Extortion

The application is based on these facts:  
See Attached Affidavit☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

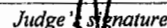
Sworn to before me and signed in my presence.

Date: May 18, 2018City and state: Charleston, South Carolina

Applicant's signature

SA Richard B. Starnes, USAC/DC

Printed name and title

  
Judge's signature

Bristow Marchant, U.S. Magistrate Judge

Printed name and title



IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF SOUTH CAROLINA  
CHARLESTON DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
EMAIL ACCOUNTS  
wilkinswendell870@gmail.com AND  
richhomiefive@gmail.com  
MAINTAINED BY GMAIL STORED AT  
PREMISES CONTROLLED BY GOOGLE,  
INC.

Case No. 2:18-CR-905

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Richard B. Starnes, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain Google email accounts that are stored at premises owned, maintained, controlled or operated by Google, Inc. ("Google"), an internet services company that provides email services (known as Gmail) headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information (including the content of communications) pertaining to the subscribers or customers associated with the user IDs, further described in Section I of Attachment B. Upon receipt of the information described in Section I of

RB3

Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B as outline in Attachment C.

2. I am a Special Agent ("SA") with the Computer Crime Investigative Unit ("CCIU"), U.S. Army Criminal Investigation Command ("USACIDC"), and have been so employed since April 2015. The primary mission of the CCIU is to investigate computer-related offenses including child pornography, extortion, computer intrusions, denial of service attacks and other types of malicious computer activity directed against the U.S. Army or conducted using Army computers. As a Special Agent of USACIDC, I am authorized to investigate crimes involving all violations of the Uniform Code of Military Justice, and other applicable federal and state laws where there is an Army interest. I have successfully completed the U.S. Army Criminal Investigation Division's Special Agent Course located at the U.S. Army Military Police School, Fort Leonard Wood, MO, which is a federally accredited criminal investigator training program. During my training at the Special Agent Course, I received legal instruction and advanced formal training on a variety of criminal investigations such as identity theft, mail fraud, bank fraud, extortion, child pornography and other related offenses. I have completed the Network Intrusion Basics Course, Introduction to Networks and Hardware, Computer Incident Response Course, and the Windows Forensic Examiner Course through the Defense Cyber Investigations Training Academy ("DCITA"). I have also completed the Digital Evidence Acquisition Specialist Program, which is a federally accredited training program located at the U.S. Federal Law Enforcement Training Center. Additionally, I have completed CID Special Agent courses that include the Special Victims Training Program, the Criminal Intelligence Training Program, Hostage/Crisis Negotiator Level One Training Course, the U.S. Army Special Forces Technical Exploitation Course, and the BATF Level One Post-Blast Investigation Course. Prior to my position with

BBS

CCIU, I was employed as a Police Officer with the Charlotte-Mecklenburg Police Department for approximately thirteen years where I obtained my basic and advanced law enforcement certificates for the State of North Carolina. My duties as an officer included the investigation and enforcement of criminal laws in the State of North Carolina. Additionally, I have served as a U.S. Army Reserve CID Special Agent since 2009. My duties as a reserve U.S. Army CID Special Agent included investigating general crimes (to include but not limited to murder, sexual assaults, various forms of fraud and related offenses) as well as conducting technical sensitive site exploitation in the war on terror.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 873, Extortion; 18 U.S.C. § 1343, Wire Fraud; and 18 U.S.C. § 880, Receiving Proceeds of Extortion, have been committed by Wendell Wilkins and the subscriber/user of email address richhomiefive@gmail.com. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes as described in Attachment B.

### JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. See 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### TECHNICAL BACKGROUND

7. E-mail and web hosting companies, such as Google, provide e-mail, webhosting, and other services to the public. Google maintains computers that are connected to the Internet, and their subscriber/customers use those computers to, among other things, send and receive e-mail and operate websites that are available to others browsing the World Wide Web.

8. E-mail providers’ customers place files, software code, databases, and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by the web hosting company. It is frequently also possible for the customer to directly access the server computer through the Secure Shell (“SSH”) or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol (“FTP”). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses (“IP addresses”) of the remote users’ computers (IP addresses are used to identify computers connected

RBj



to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

9. The servers use those files, software code, databases, and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language ("HTML") (a markup language for web content), Cascading Style Sheets ("CSS") (a language for styling web content), JavaScript (a programming language for code run on the client's browser), and image files. Web hosting companies frequently allow their customers to store collections of data in databases. Software running on the web server maintains those databases; two common such programs are named MySQL and PostgreSQL, although these are not the only ones.

10. Web sites deliver their content to users through the Hypertext Transfer Protocol ("HTTP"). Every request for a page, image file, or other resource is made through an HTTP request between the client and the server. The server sometimes keeps a log of all of these HTTP requests that shows the client's IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of Web browser the client uses.

11. In some cases, a subscriber or user will communicate directly with an e-mail provider about issues relating to an e-mail account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the company's support services, as well records of any actions taken by the company or user as a result of the communications.

#### **STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS**

12. Title 18, United States Code, Sections 2701 through 2712, is entitled "Stored Wire and Electronic Communications and Transactional Records Access." Title 18, United States Code, Section 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

13. Title 18, United States Code, Section 2703(b) provides, in relevant part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant . . . .

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –

RB

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

14. The government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service from a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(3).

15. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter –

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.

16. Title 18, United States Code Section 2510, provides, in part:

(1) “contents,” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

RB5



(2) "electronic communications system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(3) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .

(4) "electronic storage" means –

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

17. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and any data storage facility or communications facility directly related to or operating in conjunction with such device.

#### **BACKGROUND CONCERNING EMAIL**

18. In my training and experience, I have learned that Gmail provides a variety of on-line services, including electronic mail ("e-mail") access to the public. Gmail allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Gmail. During the registration process, Gmail asks subscribers to provide basic personal information. Therefore, the computers of Gmail are likely to contain stored electronic communications (including retrieved and

unretrieved e-mail for Gmail subscribers) and information concerning subscribers and their use of Gmail services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. A Gmail subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Gmail. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

20. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage

of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

22. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

23. This application seeks a warrant to search all responsive records and information under the control of Gmail, a provider subject to the jurisdiction of this court, regardless of where Gmail has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Gmail's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.<sup>1</sup>

---

<sup>1</sup> On March 23, 2018, the CLOUD Act (Clarifying Lawful Overseas Use of Data) was enacted, which requires Internet Service Providers to comply with search warrants for electronic communications regardless of whether such communication is located within or outside the United States. See Pub. L. 115-141.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

BS

**PROBABLE CAUSE**

25. This investigation is a result of investigative endeavors regarding Operation Surprise Party, a Department of Defense joint task force involving the extortion of U.S. military service members, which began in 2015. The premise of the extortion scheme follows a basic outline with several caveat movements. The extortion works when a victim meets the subject on a dating application (most often Plentyoffish). The subjects, who are inmates in the South Carolina Department of Corrections, typically pretend to be a female around the same age as the victim. Once making contact on the dating application, the conversations are transferred to phone-to-phone text messaging. After several hours to several days of texting, the subject will either send unsolicited nude images of a female to the victim and/or agree to trade sexually explicit images with the victim. After sending such images, the subject will send a text message to the victim posing as the female's father. The "father" then notifies the victim that the female is under the age of 18. The father will typically state that he will leave law enforcement out of the equation if the victim agrees to pay for various things like cell phone replacement, counseling, hospital treatments, etc. Often the victim will pay out of the fear that they will lose their careers (our victim sets are military service members) as there are compounding issues of conduct unbecoming and the fear that the victim truly believes they are in possession of child pornography and/or involved in the distribution of pornography to a child. Based on the investigation, this scheme is played out by countless prisoners housed in various facilities within the South Carolina Department of Corrections.

26. The Department of Defense Joint Counter Extortion Task Force is currently located in Charleston, South Carolina after NCIS spearheaded the effort to conduct a large-scale group one operation targeting the extortion of military service members.



27. Ms. Jalisa Thompson was identified as an individual responsible for acting as a money mule (one who receives and redistributes currency extorted from military service members) as the victims have been directed to send her the funds via a money transfer service once the extortion act occurs. In response to the blackmail/extortion described above, several military victims stated that they wired funds to a person named Jalisa Thompson during the scheme. Financial records confirm these wires to Jalisa Thompson.

28. During an interview with agents conducted on 6/7/17, Ms. Jalisa Thompson stated that she met a man she knew as "Dre", circa 2016 who was currently incarcerated at Broad River Correctional Institute in Columbia, SC. Ms. Thompson and "Dre" communicated via cell phone and Facebook. "Dre" used a Facebook account utilizing moniker "Ben Frank". Ms. Thompson stated that she assisted "Dre" by picking up money for him, which was sent via Wal-Mart to Wal-Mart and Western Union. At his direction, Ms. Thompson would take the money and load it onto prepaid credit cards or deposit it into other South Carolina Department of Corrections inmates' J-Pay accounts. She did not know the exact illegal activity "Dre" was involved in, but she knew he was involved in something apparently nefarious.

29. At the time she was assisting him, Ms. Thompson was pregnant and she could not always pick up the money. She had her child's father, Mr. Kenshuwn Goode, and her cousin Mr. Brandon Thompson pick up money for "Dre" when she could not do so. Ms. Thompson provided consent for an agent to review the text messages between herself and "Dre" on her phone and take photos of those texts and images. Among those was a text message Thompson received on 7/27/16 at 3:17 AM, in which "Dre" provided the email address, wilkinswendell870@gmail.com, and password, ALLAHAKBAR. In a text received on 8/29/16

AT 2:42 pm, Ms. Thompson received the following text, "Ayo Renada don't get off work till 5:45p.m."

30. During an interview with agents conducted on 10/5/17, Ms. Thompson stated that sometime in 2015 Wendell Wilkins, who she had known as "Dre" prior to his incarceration, connected with her on Facebook and they began communicating back and forth. At that time, Ms. Thompson was aware that Mr. Wilkins was incarcerated for robbery. Ms. Thompson and Mr. Wilkins originally communicated through Facebook Messenger. Ms. Thompson's Facebook profile was in her name. Mr. Wilkins' Facebook profile was in the name of "Ben Frank." In the past, he also used Facebook profiles in his name, as well as moniker "Askari Red Mecca".

31. Ms. Thompson provided consent for an agent to review the text messages between herself and Mr. Wilkins on her phone and take photos of those texts and images. Among those text messages were two photos of emails sent from Green Dot Corporation to richhomiefive@gmail.com. The first email stated that \$275.00 was sent from a military service member victim on 9/28/17 to richhomiefive@gmail.com. The second email stated that transaction had been cancelled. Ms. Thompson also accessed Facebook on her phone where she showed agents Mr. Wilkins' Facebook profile in the name of "Ben Frank" and allowed them to take pictures of the profile. At some point during Ms. Thompson's communications with Mr. Wilkins, he asked her to pick up money for him. Ms. Thompson did this from 2015 until late 2016 or early 2017. Initially, Ms. Thompson allowed Mr. Wilkins access to her PayPal account. The email address linked to her PayPal account is lady\_jt2@yahoo.com@yahoo.com. Mr. Wilkins had total control of the PayPal account and used it to have money sent to him.

32. Ms. Thompson stated she last spoke to Mr. Wilkins through Facebook Messenger a few weeks prior to 10/5/17. In his message to her, Mr. Wilkins asked Ms. Thompson to take his

RBS

mom to Wal-Mart. Regarding email wilkinswendell870, Jalisa Thompson received this email address with password from Wendell Wilkins to assist in the scam by receiving funds from victims. Email richhomiefive@gmail.com was found in text messages to Jalisa Thompson from Wilkins, which was found to be receiving funds from victims

33. Based on the information obtained during the interviews of Ms. Thompson, preservation letters were served on Google, Inc. In general, an email that is sent to a Gmail subscriber is stored in the subscriber's "mailbox" in Gmail's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Gmail's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Gmail's servers for a certain period of time.

#### **INFORMATION TO BE SEARCHED AND ITEMS TO BE SEIZED**

34. This warrant will be executed under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. As fully set forth in Attachment C, the information that is within the scope of Attachment B may be copied and retained by the United States; however, any information that does not fall within the scope of Attachment B will be sealed, and law information will not further review that information absent a Court order.

**CONCLUSION**

25. Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, Inc. who will then compile the requested records at a time convenient to it, there exists good cause to permit the execution of the requested warrant at any time in the day or night.

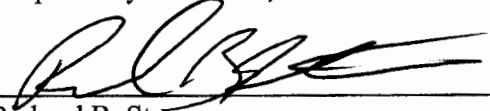
26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

27. This affidavit has been reviewed by Assistant United States Attorney Rhett DeHart.

**REQUEST FOR NON-DISCLOSURE ORDER**

28. Because notification of the existence of this order will seriously jeopardize an investigation, I request that the Court issue an order pursuant to 18 U.S.C. § 2705(b) ordering Gmail not to notify any person of the existence of the warrant.

Respectfully submitted,

  
\_\_\_\_\_  
Richard B. Starnes  
Special Agent  
USACIDC

Subscribed and sworn to before me on May 18, 2018

  
\_\_\_\_\_  
THE HONORABLE BRISTOW MARCHANT  
UNITED STATES MAGISTRATE JUDGE

